02.06.2025

Dear European Data Protection Board,

I would like to begin by expressing my sincere appreciation to you for your continued openness and commitment to stakeholder engagement. It is especially meaningful for those of us working at the intersection of blockchain technology and data protection to have a voice in shaping the interpretation of the regulation. By actively considering the perspectives of professionals in emerging and complex fields like blockchain, you demonstrate not only its dedication to inclusive dialogue but also your responsiveness to technological innovation. This collaborative approach is vital to ensuring that regulatory guidance remains both practical and forward-looking.

In this opinion piece, I offer a focused review of your recent *"Guidelines 02/25 on processing of personal data through blockchain technologies"*, specifically as it relates to the unique challenges and nuances presented by blockchain technology. My comments are limited to a few key areas where clarification and further dialogue are particularly important: encryption and confidentiality, controllership, governance, data subject rights, and the Board's overarching recommendations in public blockchains. These topics represent core aspects of the interplay between blockchain systems and data protection obligations, and I hope this contribution supports a constructive and ongoing conversation.

1. Encryption / Confidentiality

The EDPB highlights that encryption is a crucial security measure for storing personal data on blockchains, ensuring that data is only accessible to those holding the corresponding keys. However, encryption alone does not exempt controllers from GDPR obligations, as encrypted data remains personal data and is vulnerable over time due to evolving decryption methods and the indefinite retention characteristic of blockchains.

Confidentiality in blockchain depends heavily on the type of blockchain used—public or permissioned—and the mechanisms applied both on- and off-chain, such as encryption, commitments, and secure off-chain data handling. The blockchain's integrity relies on consensus protocols and the incentivization of trustworthy nodes rather than enforced trust, with additional security strengthened through certified software and node identification where applicable.

To mitigate risks linked to algorithm failures, vulnerabilities, or compromised wallets, the EDPB recommends implementing robust technical and organizational measures including emergency plans for swift response, incident notifications to supervisory authorities and data subjects, and continuous trustworthiness checks of participants.

Recognizing the limited lifespan of encryption systems, the guidance emphasizes proactive risk management throughout the data processing lifecycle. Controllers should anticipate obsolescence of cryptographic algorithms, plan for enhancements or transitions to more secure technologies, and

periodically reassess risks—especially considering emerging threats like quantum computing—to ensure ongoing protection of personal data on blockchains.

Having summarized the EDPB's position on encryption and confidentiality, I now turn to a more detailed reflection on the specific aspects that are particularly relevant within this aspect.

The following section provides my observations and commentary on key points raised in the guideline.

1. ***While encryption is a valuable security tool, blockchain systems rarely store plaintext data on-chain and blockchain's inherent cryptographic features and off-chain encryption help protect personal data and reduce privacy risks.***

While I support the use of encryption as a security measure for data stored on-chain, it is important to clarify that blockchain systems typically do not store plaintext data by default. Most commonly, only transaction data is processed and recorded on-chain. However, there are exceptions where developers may embed messages or attachments within smart contract code. In such cases, this content is often not encrypted and can be publicly accessible.

Moreover, implementing encryption for on-chain data presents several challenges. It may lead to increased gas fees, thus raising operational costs. There are also technical limitations to consider—particularly the fact that smart contracts cannot directly process encrypted data without off-chain decryption mechanisms. This reliance can compromise automation and hinder the efficiency of decentralized applications.

It is also important to recognise that blockchain technology inherently incorporates cryptographic techniques, which already serve as a strong risk mitigation measure. When encrypted data is processed off-chain and later stored or referenced on-chain, the contents of that data remain protected and are not directly visible. However, the transaction containing the encrypted data—such as metadata or references—will still be publicly accessible on the blockchain. While elements like wallet addresses or transaction hashes may still qualify as personal data under the GDPR, the use of encryption and pseudonymization significantly limits the risk of identifying individuals. As a result, the overall risk to data subjects is reduced.

2. ***Blockchain's built-in cryptographic mechanisms inherently pseudonymize personal data and offer structural security benefits that differ from traditional systems—particularly in how encryption and key management function—making some conventional data protection assumptions, like key deletion, impractical in this context.***

Blockchains inherently rely on cryptographic techniques—such as SHA-256 hashing—which serve to pseudonymize personal data by default. This cryptographic layer ensures that personal data, when processed on-chain, is not stored in plaintext and cannot be easily attributed to an individual without additional information. Importantly, this process occurs automatically as part of the blockchain protocol, without requiring a separate encryption process to be initiated by a controller or processor. The corresponding decryption capability, where applicable, is tied to the private key held within the user's digital wallet.

There are two main, most-commonly-used-types of wallets: custodial and noncustodial. Custodial wallets are operated by regulated entities, such as financial institutions or service providers, who manage and secure users' private keys using robust infrastructure—often involving Hardware Security Modules (HSMs) located in protected data centres. In contrast, noncustodial wallets give full control—and responsibility—over private keys to the user. The security of these wallets depends on the user's operational hygiene and the resilience of the wallet software or hardware. Private keys (which function as decryption keys and essentially are the wallet) cannot be deleted from the blockchain once created; they simply become inaccessible if compromised or if the user loses the seed phrase or password. Therefore, proposed solutions such as rendering encrypted data unintelligible by deleting the decryption key are, in the context of wallets, impractical and unrealistic.

While the EDPB rightly notes that encryption is not a permanent safeguard—particularly in the face of advancing technologies such as quantum computing—this is a broader concern that applies to all forms of encrypted data, not just data stored on blockchain. In fact, the risk may be more pronounced in traditional centralised systems and data centres, where there is limited transparency into how data is processed, stored, or deleted. Even though such facilities may undergo audits, full assurance regarding the secure and irreversible deletion of data is often not possible. Blockchain, by contrast, offers a decentralised trust framework, where verification is not dependent on a single provider's assurances, but is instead built into the structure and consensus mechanisms of the network.

3. ***The openness of public blockchains is a deliberate and valuable feature—not a flaw—and privacy can be effectively protected by designing systems that avoid storing personal data or use pseudonymization in alignment with blockchain's decentralised architecture.***

Critics often highlight that public blockchains are inherently permissionless and accessible to anyone. However, this openness is not a flaw but a defining feature that ensures transparency, data availability, and security through decentralised verification. In such networks, it is technically not feasible to restrict the broadcasting of transaction data to specific participants. Public blockchains are intentionally designed to be censorship-resistant, meaning that once data is submitted, it is propagated across the network without discrimination or gatekeeping.

Given these characteristics, a more practical and privacy-conscious approach would be to design smart contracts in a way that avoids the inclusion of personal data altogether. Where this is not possible, data should be structured in a pseudonymized form, ensuring that only the parties directly involved in a transaction have access to the additional contextual information necessary to re-identify an individual. This approach upholds the principles of data minimisation and purpose limitation while remaining consistent with the technical architecture and governance model of public blockchains.

4. ***While public blockchains inherently offer confidentiality through pseudonymization, this protection can be weakened when off-chain identity data—collected for regulatory compliance like KYC/AML—is combined with on-chain analytics, enabling re-identification of users.***

It is important to note that public blockchains provide a baseline level of confidentiality through pseudonymization, as personal data is not stored in plain text and users are represented by alphanumeric wallet addresses. In this sense, confidentiality is inherent to the design of public blockchains.

However, this confidentiality can be undermined by external regulatory and compliance requirements, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations. These rules often require financial institutions and service providers to collect, store, and process identifying information off-chain. When combined with blockchain analytics and chain intelligence tools, this additional

context can re-establish the link between on-chain pseudonymous identifiers and real-world identities. As a result, while the blockchain protocol itself may support confidentiality, it can be compromised by external data aggregation practices carried out for regulatory or law enforcement purposes.

5. ***Public blockchains establish trust through code and consensus mechanisms rather than personal identities, making the system "trustless" by eliminating the need to trust individual participants and relying instead on decentralized, programmatic enforcement of security and integrity.***

It is important to recognise that in public blockchains, trust is established through code and cryptographic consensus mechanisms rather than through personal relationships or identifiable actors. This is why such systems are often described as "trustless"—not because they lack trust, but because they eliminate the need for trust in individual participants. By design, it is not feasible to identify or continuously verify all actors participating in a public blockchain network. Instead, security and integrity are enforced programmatically through open-source protocols, economic incentives, and decentralized governance.

6. ***Decentralized public blockchains lack a traditional GDPR-style controllership model, making it challenging to assign responsibility and fulfil accountability and compliance obligations due to distributed governance and the consensus-based nature of decision-making.***

A key challenge in the context of blockchain is the absence of a traditional controllership model as envisioned by the GDPR. In decentralized public blockchain systems, there is often no single entity with the authority or responsibility to implement emergency plans, disclose vulnerabilities, or coordinate breach notifications. Governance is distributed across a network of participants, and decisions—such as updating algorithms or responding to security incidents—typically require consensus, which can be complex and time-consuming to achieve. This raises important questions about how accountability and compliance obligations can be meaningfully fulfilled in such decentralized environments.

7. ***Wallet security is essential to prevent unauthorized blockchain transactions, with custodial wallets relying on institutional safeguards and noncustodial wallets depending on user responsibility—making robust technical and organizational protections critical in the irreversible blockchain environment.***

Wallet security is a critical factor in safeguarding against unintended or unauthorized transactions on a blockchain. As previously noted, there are two main, mostly-used-common categories of wallets: custodial and noncustodial.

Custodial wallets are typically managed by financial institutions or regulated service providers on behalf of users. These providers are responsible for securing private keys, often through the use of specialised infrastructure such as Hardware Security Modules (HSMs) within protected data centres. In these setups, robust internal controls, employee access restrictions, and incident response protocols are essential to mitigate the risk of compromise by rogue employees or external attackers.

Noncustodial wallets, by contrast, place the full responsibility for key management on the user. The security of such wallets depends heavily on user behaviour and the protective measures they employ (e.g., use of hardware wallets, secure backups, and multifactor authentication). While these wallets enhance user autonomy and privacy, they also increase the risk of loss or unauthorized transactions if private keys are compromised.

The decentralized nature of blockchain means that, once authorised by a private key, transactions are irreversible. This highlights the importance of implementing technical and organizational safeguards—both at the infrastructure and user levels—to protect wallet integrity and prevent unauthorized use. These safeguards should form a key part of the broader data protection and security strategy for any actor participating in blockchain-based ecosystems.

8. ***The potential future obsolescence of encryption affects all digital systems, including blockchain; however, blockchain's decentralized governance makes timely updates in a traditional manner challenging, even though its inherent cryptographic design and transparency provide strong foundational security and resilience.***

The concern regarding the eventual obsolescence of encryption algorithms—particularly in light of advancements such as cryptanalytically-relevant quantum computing—is valid and applies broadly across all digital systems, not just blockchain. This is not a blockchain-specific vulnerability, but a universal challenge affecting all encryption-based security frameworks, including those used in traditional centralised data infrastructures.

However, the application of these concerns to blockchain must take into account the unique governance and architectural model of decentralized networks. As previously noted, public blockchains do not operate under a classical controllership model as envisioned by the GDPR. There is typically no single entity with authority over the entire system who can conduct periodic reassessments, implement updates to encryption protocols, or migrate processing to new technologies unilaterally. Governance is distributed, and protocol changes often require consensus across a diverse and global set of participants—making centralised risk management strategies difficult to implement in practice.

That said, blockchain systems do incorporate robust cryptographic mechanisms by design, including hashing and pseudonymization, which offer meaningful baseline protections. While no encryption can guarantee perpetual security, the decentralized and transparent nature of blockchain reduces reliance on opaque third-party systems and can help build resilience.

2. Controllership

The EDPB acknowledges that **nodes in public, permissionless blockchains** may engage in various data processing activities and that **their role as controllers or joint controllers** depends on their influence over the purposes and essential means of the processing. In some cases, nodes may act independently and even pursue their own objectives—such as through **transaction selection or protocol modifications (e.g. forks)**—without acting on instructions from any central party. In such scenarios, they may be deemed controllers under the GDPR.

To address the complexities of decentralized control, the EDPB encourages the **creation of a legal entity or consortium** among nodes. If established, this consortium would assume controllership responsibilities for the processing activities carried out on the chain.

The EDPB further emphasizes that controllers must **evaluate the publicity and nature of the data** involved in processing, particularly when deciding whether to use a **public or non-public blockchain**. Public blockchains should only be used where transparency is necessary for achieving a specific processing purpose, and **personal data should be minimized and not directly stored on-chain**.

In line with the **data minimization principle**, only essential personal data should be processed on the blockchain, and **technical and organizational measures (TOMs)** must ensure that by default, data

is not accessible to an indefinite number of people without the data subject's intervention (Article 25(2) GDPR).

The **international nature of blockchain networks** also raises data transfer concerns, as **nodes are not pre-selected or vetted**, and their global distribution can trigger cross-border transfers. Controllers must comply with **Chapter V GDPR**, identifying such transfers and implementing mechanisms like **standard contractual clauses**—though EDPB acknowledges this may be difficult in permissionless environments.

Finally, the EDPB highlights that data uploaded to the blockchain should be minimized (Recital 88), and that **default exposure of personal data on public chains should be prevented** unless the data subject has intervened directly (Recital 118). Additionally, the **technical resilience and cryptographic integrity** of blockchain systems must be maintained, with contingency plans in place for potential algorithmic failures (Recital 85).

The following section provides my observations and commentary on key points raised in the guideline.

1. ***Nodes in public blockchains are essential infrastructure components that validate and propagate transactions without controlling or determining how personal data is processed, meaning they do not qualify as controllers or processors under the GDPR—the responsibility lies with the users who initiate the transactions.***

Public blockchains operate through a globally distributed and decentralised network of nodes, each responsible for maintaining the functionality and security of the system. The primary role of nodes is to listen for incoming transactions, group them into blocks, and participate in the validation or mining of new blocks. By performing these functions, nodes collectively secure the network and ensure its continuous operation.

Importantly, nodes operate strictly according to the predefined rules encoded in the blockchain protocol. They do not initiate transactions, nor do they exercise discretion over which transactions are processed or broadcasted. Their participation is limited to validating and propagating data submitted by users.

Since nodes do not determine the purpose or means of processing personal data on the blockchain, they do not exercise decisive influence over the data processing activities. Furthermore, nodes do not act on behalf of any controller and therefore cannot be classified as processors either. Instead, they serve as essential components of the blockchain infrastructure that maintain and secure the network. Without the nodes, the blockchain would not function. The responsibility for deciding the purposes and essential means of processing personal data rests solely with the users—natural or legal persons—who initiate and control the transactions on the blockchain.

2. ***Although nodes in public blockchains can influence transaction inclusion, they do not determine the purposes or essential means of personal data processing as required under the GDPR, and thus should not be considered controllers—even when acting collectively—highlighting the need for clearer regulatory guidance tailored to decentralized environments.***

It is accurate that nodes or validators in public permissionless blockchains can make decisions regarding forks or the inclusion or exclusion of specific transactions[1] (e.g., Tornado Cash transactions[2]). However, these decisions do not equate to determining the purposes and essential means of personal data processing as defined under the GDPR. As such, nodes should not be considered controllers—even in cases where a consortium or legal entity is formed among them.

Under the GDPR, a controller is a natural or legal person who determines the purposes ("why") and essential means ("how") of personal data processing. In the context of public blockchains, it is the users—natural or legal persons—who determine the purpose of processing by choosing to use the blockchain for a given transaction. They also influence the means by submitting specific data in a manner consistent with the protocol's design.

Nodes, on the other hand, perform a protocol-defined function: they validate, propagate, and store data. While they may choose whether to include certain transactions in a block (such as filtering based on compliance risk or local regulatory pressure), this influence is limited to execution at the block level and does not rise to the level of controlling the processing activity in a GDPR sense. They do not determine *why* personal data is processed, nor do they control the types of personal data submitted or the identity of the data subjects.

Furthermore, in public permissionless blockchains, nodes typically do not know or coordinate with one another. These nodes are geographically dispersed and often pseudonymous, which makes sustained coordination extremely difficult. Even if node operators attempted to organise through a consortium, practical and technical constraints—such as consensus rules, protocol-level immutability, and the decentralized architecture—would render such efforts largely ineffective in managing or controlling data processing activities. Thus, the idea of collective controllership via a node consortium is not viable in public blockchain environments.

The EDPB itself states that determining the purposes and essential means of processing requires a level of control over elements such as the type of data processed, retention periods, access rights, and categories of data subjects. Nodes do not have control over these factors. Their role is better understood as protocol enforcers rather than decision-makers in the data protection sense.

Therefore, there is a pressing need for clearer regulatory guidance on how much influence over the "why" and "how" of processing is required to qualify as a controller, especially in decentralized environments where roles and responsibilities are fundamentally different from traditional centralised models.

3. ***While minimizing on-chain personal data is a sound principle, public blockchains—especially in DeFi—require certain pseudonymous data (like wallet addresses) to function, making some data processing unavoidable; regulatory guidance should therefore adopt a nuanced, risk-based approach that reflects the technical and operational realities of decentralized systems.***

I generally support the EDPB's recommendation to avoid storing personal data on-chain and to carefully assess the level of publicity associated with blockchain transactions. However, it is important to acknowledge that this recommendation may have practical limitations in certain contexts—particularly with regard to smart contract functionality and decentralized finance (DeFi) platforms.

---

[1] A tool to observe OFAC compliant blocks on Ethereum - https://www.mevwatch.info/
[2] Please see for more details on the Tornado Cash law suit in the Netherlands: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Oost-Brabant/Nieuws/Paginas/Developer-of-Tornado-Cash-gets-jail-sentence-for-laundering-billions-of-dollars-in-cryptocurrency.aspx

In many blockchain-based systems, certain personal data—such as wallet addresses—are inherently part of the transaction logic and are publicly broadcasted on the chain. These identifiers, while pseudonymized, may still fall within the scope of personal data under the GDPR. In the context of DeFi, there is typically no flexibility for the controller (the user) to choose the blockchain architecture, as decentralized applications (dApps) and protocols are already deployed on specific chains. Users interact with these dApps by connecting their wallets, which inherently involves the inclusion of pseudonymized identifiers in transaction data.

This is not a design flaw, but a core characteristic of public blockchains—transparency is fundamental to their operation and to the verification of transaction integrity. As a result, a certain degree of pseudonymous data processing must be accepted as a necessary feature of using such infrastructure.

That said, privacy-enhancing tools do exist and can offer additional safeguards. For example, mixers are designed to obfuscate transaction trails by allowing users to deposit and withdraw funds in a manner that breaks the link between sender and recipient. While these tools serve a legitimate privacy-preserving function, their use has become legally controversial. Bodies such as the Financial Action Task Force (FATF) have flagged mixers as high-risk instruments due to their potential misuse in money laundering and sanctions evasion[3] .

Therefore, while we agree with the general principle of minimising on-chain personal data, regulatory guidance must also account for the technical constraints and functional realities of decentralised ecosystems. A nuanced, risk-based approach—rather than a blanket prohibition—will be essential for balancing data protection with innovation in decentralised technologies.

4. ***Public blockchains are transparently designed public infrastructures where pseudonymized personal data is inherent and often user-controlled, so applying traditional data protection concepts like strict access limitations risks conflicting with the foundational principles of decentralisation—calling for a more contextual, technology-aware regulatory approach.***

Public blockchains function as public infrastructure—open, decentralized systems designed to serve as verifiable ledgers for on-chain activity. Their transparency is not a byproduct but a foundational principle. The ability for anyone to inspect transaction histories ensures integrity, auditability, and trust in the system. This openness is a feature, not a flaw, and is essential for ensuring decentralized consensus and preventing tampering or censorship.

From this perspective, the fact that personal data—such as wallet addresses—is accessible on-chain may appear counterintuitive under traditional data protection frameworks. However, personal data on public blockchains is generally pseudonymised by default. Technical and organisational measures (TOMs) are embedded within the design of the system: wallet addresses are not directly linked to real-world identities, and absent additional context, such as Know Your Customer (KYC) data held by third parties or a user's voluntary public disclosure, it is not possible for the average person browsing the blockchain to identify an individual.

Requiring additional TOMs beyond what is inherent to the protocol may in some cases undermine the self-determination principle of decentralized systems. For example, if a user publicly associates their wallet address with their identity—whether for business, reputation, or transparency purposes—they

---

[3] Please see for further information on FATF's guidance in terms of mixers and tumblers and its flagging of anonymity tools red.
https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-VA-VASPs.pdf
https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

are exercising autonomy over their personal data. In such cases, additional access restrictions could contradict the user's own choice to operate publicly within a transparent system.

While we agree that processing of personal data must be lawful and proportionate, applying conventional access-limitation standards to public blockchains risks misaligning with the underlying technology and its governance. A more contextual approach is needed—one that recognises the pseudonymous nature of on-chain data, the decentralised allocation of roles and responsibilities, and the voluntary, permissionless participation of users in these systems.

5. ***Applying the GDPR's data minimisation principle to public blockchains requires a context-aware approach that respects the decentralised architecture, recognises users as the controllers of their own data, and acknowledges that key protocol functions depend on processing a minimal, essential set of pseudonymized data points—making classical, centralised interpretations of controllership and minimisation impractical.***

The data minimisation principle, as outlined in the GDPR, is certainly achievable in private or permissioned blockchain environments, where participants and governance structures are predefined and centralised. However, in the context of public blockchains, the situation is fundamentally different and requires a tailored interpretation.

In public permissionless blockchains, the concept of classical controllership does not neatly apply. The users themselves—by voluntarily initiating transactions—should be considered the controllers, as they are the ones deciding both the purpose and the means of the data processing. Interfaces, wallets, or other intermediaries merely provide access to the protocol and do not determine *why* or *how* personal data is processed. They therefore do not meet the criteria of a controller under Article 4(7) GDPR.

Accordingly, the obligation to ensure data minimisation cannot reasonably be transferred to nodes or access providers, who neither initiate transactions nor influence their content. Public blockchain protocols process a very limited and specific set of data points: wallet addresses (pseudonymous identifiers), smart contract addresses, transaction values, timestamps, and function-specific parameters. These are essential for ensuring the validity, ordering, and execution of transactions within a decentralised system. Unlike many traditional or AI-driven systems, blockchains do not collect expansive metadata or behavioural profiling information.

Furthermore, publicity in public blockchains is intrinsic to their function. It is not a design flaw, but a foundational feature necessary to ensure decentralized consensus, prevent tampering, and enable open verification. Users choose to participate in this public infrastructure, and their conscious decision to broadcast data—often pseudonymized—is an exercise of digital autonomy that should not be misattributed to other actors.

Therefore, applying a strict, centralised interpretation of the data minimisation principle to decentralized networks risks misaligning regulatory expectations with technical realities. A more context-aware approach is needed—one that recognises the role of individual agency and the inherent limitations and affordances of public blockchain technologies.

6. ***Applying Chapter V GDPR's international data transfer rules to public blockchains is impractical due to their decentralised, pseudonymous, and globally distributed nature, making traditional mechanisms like SCCs unworkable—necessitating a more nuanced, risk-based approach tailored to blockchain's structural realities.***

The application of Chapter V GDPR to public blockchains presents significant challenges due to the absence of classical controllership and the decentralised nature of the infrastructure. In public permissionless blockchains, it is not possible to establish or enforce contractual agreements—such as Standard Contractual Clauses (SCCs)—with all participating nodes globally. Nodes are not pre-selected or vetted, and they can join or exit the network at any time, often pseudonymously and without geographic restrictions.

Once a transaction is broadcast to the blockchain, it is propagated across a distributed network of nodes worldwide. In proof-of-stake (PoS) systems, for instance, it is not known in advance which node will validate the next block, nor is it possible to determine from which jurisdiction the transaction originates or to which jurisdictions it will be replicated. This unpredictability and global replication are core design features of decentralised systems.

While it is true that this results in international data transfers, these flows are intrinsic to the operation of public blockchains. Attempting to apply traditional cross-border transfer mechanisms designed for centralised environments to decentralised networks may lead to impractical or unworkable compliance expectations. As such, a nuanced approach is needed—one that recognises the structural differences of blockchain technology and focuses on risk-based safeguards at the protocol and application layers, rather than trying to retrofit contractual mechanisms onto a decentralised infrastructure that operates without central control.

7. ***The blockchain ecosystem already embraces robust, transparent, and proactive software development and security practices—such as audits, formal verification, and bug bounties—which effectively address many of the EDPB's concerns about long-term risk and reliability in decentralised systems.***

Robust software development practices—such as quality assurance (QA), code audits, peer reviews, and formal verification—are already widely adopted across the blockchain ecosystem. These measures are part of standard industry practice and are crucial for maintaining security and reliability, particularly in projects with high-value or high-risk use cases.

Leading blockchain projects routinely engage independent third-party auditors to assess both the cryptographic algorithms and their implementation in smart contracts and protocol code. In many cases, these audit results are publicly disclosed, reinforcing transparency and trust within the community. Additionally, responsible development teams often implement bug bounty programs and coordinate responsible disclosure mechanisms to catch vulnerabilities early.

While the EDPB's concern is valid—especially considering the long lifespan of blockchain infrastructures—the blockchain community has already internalised many of these risk mitigation strategies as part of its technical culture. Continuous assessment and upgrades are aligned with the fast-evolving nature of cryptography and are an integral part of open-source blockchain development cycles.

8. ***In decentralised public blockchains, users—not nodes or technical participants—determine the purpose and means of data processing, meaning classical GDPR controllership and data minimisation obligations cannot reasonably be applied to infrastructure actors who simply follow protocol rules without influencing the content or purpose of the data.***

In decentralized systems, the concept of classical controllership—centralised authority over the purpose and means of data processing—does not apply in the traditional GDPR sense. In public blockchains, there is no single entity that determines which data is uploaded or how it is processed by the network. Instead, individual users independently and voluntarily choose to broadcast transactions

to the blockchain. As such, they are the ones determining the purpose and means of processing their own (often pseudonymized) personal data.

Accordingly, it is not feasible to impose data minimisation obligations on nodes or other technical participants, who do not originate or modify the data they process. These actors operate based on the protocol's rules and do not have a role in determining the purpose or overall content of the data submitted by users. While nodes may choose not to validate certain transactions—such as those previously flagged for compliance or legal concerns—this selective validation occurs at the execution layer and does not equate to exercising control over the nature of the data itself. Their limited discretion does not rise to the level of controllership as defined under the GDPR.

9. ***In public blockchains, the data subject often acts as the controller by voluntarily broadcasting their data, meaning GDPR requirements around data accessibility without the subject's intervention are already met—so imposing additional safeguards is both redundant and incompatible with the transparency and user autonomy central to decentralised systems.***

This recommendation appears to misunderstand the operational realities of public blockchains. In decentralized environments, it is often the data subject themselves who initiates and broadcasts the transaction. In such cases, the data subject is also acting as the controller, deciding both the purpose and means of the processing. Therefore, the requirement that personal data should not be made accessible "without the data subject's intervention" is already inherently fulfilled.

Requiring an additional safeguard against public accessibility, in this context, is not only redundant but unrealistic. Public blockchains are designed to ensure transparency and verifiability, and data broadcast to the chain is done so with the informed and deliberate action of the user. Imposing stricter barriers would contradict the principle of user autonomy that underpins decentralized systems.

3. Governance

The EDPB emphasizes that **governance mechanisms play a critical role** in defining roles and responsibilities under the GDPR, particularly in distinguishing between **centralized and decentralized models**. Governance frameworks can be formalized on-chain or off-chain and typically encompass:

- **Technical specifications** such as formats, protocols, algorithms, and software updates
- **Organizational and legal elements** including accountability structures, contractual obligations, and data protection by design
- **Policy management**, including the handling of inconsistencies, violations, and adherence to GDPR principles

In addition, the **evolution of blockchain software and protocols**—including any changes to permissions or operational logic—**must be clearly documented**. This ensures that the implementation of changes remains aligned with intended privacy and compliance safeguards.

Overall, the EDPB expects that governance documentation and procedures will contribute to transparency, accountability, and alignment with **GDPR requirements**, especially regarding **data protection by design and default**.

My comments on the aforementioned topics are provided below.

1. ***Public blockchains are open, decentralized systems governed collectively through transparent, community-driven processes, not controlled by any single entity. Service providers and users who interact with these blockchains do not control their core design but are responsible for how they manage their own data and applications when using the blockchain.***

Public blockchains function as permissionless, decentralized infrastructures. This means that anyone can join the network, validate transactions, and deploy smart contracts without prior approval or coordination. Service providers and users operating on public blockchains do not have control over the foundational governance or technical architecture of the chain itself.

The design and evolution of public blockchains—such as Ethereum—are managed through transparent and community-driven processes like Ethereum Improvement Proposals (EIPs). These are open to public scrutiny and deliberation, primarily led by core developers and subject to decentralized consensus. Public blockchains are not offered as customisable services by a single provider, nor are they modifiable at the discretion of individual participants.

As such, centralized service providers who choose to build on or integrate with public blockchains do not define the design of the blockchain, but rather, make a conscious decision to interact with it. Within this framework, these entities retain full control over how they structure their own data flows and application logic. They are responsible for implementing appropriate technical and organizational measures (TOMs) in the way their services interface with the blockchain, including decisions around what data is submitted and how it is processed on-chain.

2. ***In public, permissionless blockchains, decentralized and community-driven governance replaces traditional centralized control, making conventional accountability frameworks—like top-down documentation of changes—impractical. Instead, transparency and accountability arise from open-source development, public participation, and consensus, which should be acknowledged in regulatory considerations.***

The recommendation lacks clarity in the context of public, permissionless blockchains, where there is no centralized governance or classical controllership as envisioned under the GDPR. In decentralized systems, software and protocol changes—such as upgrades or hard forks—are proposed, debated, and adopted through community-driven processes. These processes are transparent, open to public participation, and not controlled by a single entity.

Because of this decentralized governance model, it is not feasible to assign traditional accountability roles, such as those required to “document governance of changes” in a top-down manner. Instead, alignment between protocol design and implementation is ensured through open-source development practices, community review, and consensus-based decision-making. While this does not resemble classical organizational procedures, it provides its own form of transparency and accountability, which should be recognised in any regulatory analysis.

3. ***The recommendation to document governance of software and protocol changes is unclear and impractical for decentralized, permissionless blockchains, where protocol evolution happens through open, community-driven consensus, making the purpose and enforcement of such documentation uncertain.***

The recommendation to document the governance of software and protocol evolution lacks clarity regarding its practical purpose and applicability, especially in the context of decentralized, permissionless blockchains. Given the open and community-driven nature of protocol development, where changes are proposed, reviewed, and adopted through collaborative consensus mechanisms, it is unclear what specific benefits such documentation would provide or how it would be enforced.

4. Data Subject Rights

The EDPB emphasizes that **data subject rights under the GDPR are technology-neutral** and must be **respected even in blockchain-based systems**. However, the **immutable nature of blockchains** introduces challenges, particularly around the **right to erasure (Article 17)** and **rectification (Article 16)**.

Key points include:

- **Immutability and Erasure**: Data stored on a blockchain—whether in clear text, encrypted, or hashed form—is practically irreversible. Deleting or modifying such data is extremely difficult, often requiring coordinated action from all participating nodes. Nevertheless, the EDPB insists that **technical limitations cannot be used as an excuse** for non-compliance.

- **Storage Limitation Principle**: Personal data must be erased when the processing purpose is fulfilled and retention periods have expired. If erasure cannot occur on-chain, **off-chain architectures should be designed** to de-identify or prevent the re-identification of data subjects. Controllers must ensure that **effective deletion methods**—even at the architectural level—are in place.

- **Data Retention Justification**: The **lifetime of the blockchain** should not be the default data retention period. Controllers must assess and justify the necessity and proportionality of any retention that equals or exceeds the blockchain's lifespan, documenting this analysis.

- **Avoid On-Chain Personal Data**: The EDPB recommends that **personal data in directly identifying forms** not be written to the blockchain. Instead, it should be processed **off-chain**, where data subject rights (e.g. deletion, rectification) can be realistically exercised.

- **Innovation with Safeguards**: While **blockchain systems can explore innovative solutions** (e.g. privacy-enhancing technologies, new key management schemes) to uphold data subject rights, these must never **reduce the level of protection** provided under the GDPR. Their **effectiveness must be assessed** as part of risk management throughout the processing lifecycle.

The following section contains my remarks on the topics discussed above.

1. ***While the right to erasure is practically impossible on public blockchains due to their immutability, directly identifying personal data is rarely stored on-chain. Forks do not undermine data integrity but represent a divergence in the blockchain's history. Existing GDPR frameworks did not anticipate decentralized blockchains, highlighting the need for updated guidance and a balanced approach combining technical and governance measures.***

It is accurate that exercising the right to erasure on a public blockchain is effectively impossible due to the immutable and indefinite nature of data storage. However, storing personal data in a directly identifying form on a public blockchain is uncommon. For private blockchains, this issue can be addressed technically since controllers maintain full control over the chain.

Regarding forks, while the EDPB suggests that forking undermines the principles of consistency and tamper-proof processing, this interpretation does not fully reflect the technical reality. Forking results in a split where nodes choose which chain to follow, creating two separate ledgers with their own data sets. The original data on the previous chain remains intact and unaltered, preserving immutability. The new chain's genesis block after the fork simply timestamps the divergence. For example, the DAO hack[4] resulted in the creation of Ethereum (ETH) and Ethereum Classic (ETC) chains, both preserving historical data without retroactive modifications.

Thus, forks do not compromise tamper-proof principles but rather reflect a historical divergence in the blockchain's evolution.

While we support the EDPB's call for a proactive approach combining technical, organizational, and governance measures, it is important to remember that when the GDPR was enacted, decentralized blockchain technology was largely unaccounted for. The legislation only briefly references decentralized systems and provides no specific guidance. It may be that this was a deliberate legislative choice to exclude or limit blockchain's scope under GDPR.

2. ***Data deletion on public blockchains is technically and practically impossible due to their immutable, censorship-resistant design, conflicting with GDPR's deletion requirements. GDPR was created with centralized systems in mind and doesn't fit well with blockchain realities, especially given mandatory data retention laws and the decentralized, pseudonymous nature of nodes, which makes enforcing deletion requests unfeasible.***

Data deletion at the individual level on a blockchain is technically infeasible and fundamentally conflicts with the tamper-proof nature that the EDPB values. Deleting the entire blockchain is equally impractical, as public blockchains are architected to be censorship-resistant and resilient against such attacks, ensuring high data availability—a principle that aligns with GDPR's goals. Thus, the suggested approach appears more theoretical than realistic.

It is important to recall that the GDPR, at the time of its drafting and adoption, primarily envisioned centralized cloud systems and did not specifically address blockchain technology.

---

[4] Please see how the DAO hack resulted in an earlier hard fork on the Ethereum network: https://www.coinbase.com/en-gb/learn/crypto-basics/what-is-the-difference-between-ethereum-and-ethereum-classic

Given the significant current use of blockchain in the finance sector, combined with mandatory retention periods (e.g., 5 years under AML/KYC obligations in most jurisdictions), even a carefully designed combination of on-chain and off-chain data cannot fully prevent the future re-identification of data subjects. This is especially relevant due to EU AML rules on fund transfers and sanctions compliance.

Furthermore, controllers do not have knowledge of, nor legal relationships with, the nodes that maintain the blockchain, making enforcement of deletion requests impossible. While it is theoretically possible to refuse validation of certain transactions, these transactions remain broadcast across the network even if unvalidated. Nodes are economically incentivized to validate transactions, and absent extraordinary circumstances—such as a major update or crisis—they have little motivation to exclude data solely to comply with GDPR.

Lastly, in the pseudonymous environment of blockchains, nodes cannot ascertain whether a data subject is an EU resident whose data must be erased. This interpretation of blockchain technology and GDPR compliance does not align with practical realities and should be reconsidered.

3. ***The EDPB's expectations for data retention and deletion assume traditional data controllers who can delete data, but in decentralized public blockchains, users act as controllers and data is immutable. Therefore, standard GDPR retention and deletion rules are impractical and don't align with the technical realities of public blockchains.***

The EDPB's expectations regarding data retention and deletion presuppose classical controllership and the practical ability to delete data. However, in decentralized public blockchains, classical controllership does not apply, as users themselves determine the purpose and means of processing by broadcasting transactions.

Moreover, once data is recorded on the blockchain, deletion is not technically feasible due to the tamper-proof, immutable nature of the technology. Therefore, it is unrealistic to expect controllers—or any other party—to delete data in line with traditional GDPR retention principles.

This fundamental technical limitation calls into question the applicability of standard retention and deletion requirements to blockchain systems, especially public ones. Controllers cannot impose or enforce retention periods on blockchain data, nor can they justify retention periods based on deletion capabilities that do not exist in practice.

4. ***In public blockchains, there is no traditional data controller; users themselves act as both data subjects and controllers by choosing to broadcast their data. Therefore, the responsibility to exercise data protection rights lies with the users, not with intermediaries like wallets or nodes, reflecting the decentralized nature of blockchain.***

The EDPB's statement assumes the presence of a classical data controller responsible for ensuring data subject rights. However, as previously stated, in public blockchain contexts, classical controllership does not exist. The interfaces (wallets, dApps, nodes) facilitating access to the blockchain are not controllers; rather, the users themselves are both the data subjects and effectively the controllers, as they decide to use the blockchain and broadcast their data.

Therefore, it is the responsibility of the users/data subjects to ensure they can exercise their rights. If they do not consent to the use of public blockchains for processing their personal data, they have the option to refrain from engaging with those systems. This self-determination shifts the burden of compliance away from intermediaries and aligns with the decentralized nature of blockchain.

5. ***While it's advisable to avoid storing personal data directly on-chain, intermediaries that simply provide access to public blockchains should only be responsible for the personal data they directly process themselves, not for the data inherently stored or processed on the blockchain, since they do not control or alter that data.***

Depending on the business case, I generally support the recommendation to avoid storing personal data directly on-chain and instead keep it off-chain. However, when a business acts merely as an interface or facilitator providing access to a public blockchain, its responsibility should be limited to the personal data it processes as a controller in its own right and within the scope of its operations.

In other words, such intermediaries should not be held responsible for personal data inherently stored or processed on the blockchain itself, since they do not control or modify that data. Their accountability should be confined to their own processing activities, consistent with their role and legal establishment.

5. Recommendations

The EDPB recommends some action points below:

- **Trust through Certification (Recommendation 5)**
  Implementations should include **trust mechanisms**, such as **certified software** or **verified node identities**, ideally backed by **international standards** or **independent third-party audits**. These are meant to support accountability and reliability in blockchain environments.

- **Legal Clarity When Blockchain Use Is Mandated (Recommendation 6)**
  If **Union or Member State law mandates the use of blockchain**, legislators must clearly define what **levels of publicity are acceptable** and **how confidentiality should be protected**. Legal frameworks should discourage confidentiality breaches and tailor blockchain use accordingly.

- **Data Protection by Design and by Default (Recommendation 10)**
  All blockchain-based processing must **embed data protection principles**—like necessity, proportionality, and minimization—from the outset and throughout the processing lifecycle. Compliance must not be an afterthought but **integrated into the architecture** of any blockchain system.

- **Security- Limiting Public Access Where Not Necessary (Recommendation 15)**
  If **a public blockchain is not essential** for a processing purpose, measures must be implemented to **limit its accessibility** and ensure **confidentiality of data**. These safeguards must be **documented and verifiable**.

The following section presents my analysis and perspective on selected recommendations.

1. ***Expecting all participants in permissionless public blockchains (including anonymous, global nodes) to obtain certifications is unrealistic and contradicts the decentralized nature of these systems. Trust is derived from the open-source protocol and community governance, not from certifying individual nodes.***

The recommendation 5 is unrealistic for permissionless public blockchains. Nodes are distributed globally and often anonymous. While some organizations provide validation services as nodes, any individual — including an average user with a computer — can join and perform validation activities without centralized oversight. Expecting all such participants to obtain certifications contradicts the fundamental permissionless and decentralized nature of these blockchains.

Trust in these systems stems from the algorithm and the open-source code, which are publicly available and transparently discussed through community-driven proposals. Thus, trust is established by the technical protocol itself, not by certification of individual nodes.

2. ***The recommendation applies mainly to private blockchains with controlled governance, as public blockchains' decentralized, permissionless nature makes such mandates impractical. However, emerging privacy-enhancing technologies like zero-knowledge proofs offer promising ways to improve privacy on public blockchains without sacrificing their openness.***

This recommendation 6 is realistically applicable only to private blockchains, where governance and access can be legally mandated and controlled. Public blockchains, by their nature, cannot be mandated in the same way due to their permissionless and decentralized architecture. However, ongoing developments in privacy-enhancing technologies (PETs), such as zero-knowledge proofs (ZK proofs)[5], demonstrate that privacy solutions for public blockchains are feasible and evolving, potentially addressing concerns around publicity and confidentiality without restricting the openness of these networks.

3. ***GDPR principles were designed for centralized cloud services, not decentralized blockchains. Since blockchains already minimize data and use cryptography and pseudonymization, the EDPB should recognize these inherent privacy features and promote privacy-enhancing technologies and tailored regulatory approaches that align blockchain practices with GDPR's core goals.***

The GDPR principles were primarily written with cloud service providers in mind, not decentralized technologies like blockchains. However, blockchains already process minimized sets of data by default, employing cryptographic techniques and pseudonymization to protect personal information. If the EDPB wants these principles to be meaningfully applicable to blockchain systems, it needs to adopt a new perspective that acknowledges these inherent privacy-preserving features. Moreover, privacy-enhancing technologies ("PET"s) and regulatory equivalent solutions—where blockchain actors develop tailored approaches suitable to their systems but still achieve the GDPR's core policy goals—should be actively encouraged and incentivized.

---

[5] Some examples of privacy preserving solutions on public blockchains are:
1. Nightfall, created by Ernst & Young. - a privacy-enhancing protocol that uses zero-knowledge proofs to enable private transactions on public blockchains like Ethereum
https://blockchain.ey.com/uploads/Nightfall_Usecase.pdf
https://github.com/EYBlockchain/nightfall_3
2. Railgun project - a smart contract system that provides ZK privacy on DApps.
https://www.railgun.org/
3. 0xbow-a privacy-focused protocol that enables confidential, selective data sharing on public blockchains using zero-knowledge proofs.
https://0xbow.io/ and https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364

4. ***It is impossible to limit access to permissionless public blockchains because their open, decentralized, and immutable design ensures that once deployed, the blockchain and its smart contracts remain fully accessible and operational to anyone, regardless of restrictions on user interfaces.***

Limiting accessibility of a blockchain is simply not feasible in permissionless public blockchains. By design, these chains are fully accessible and open source—once the code is deployed, it cannot be taken down. While it is possible to restrict or geo-block access to user interfaces (UIs), the underlying smart contract code and blockchain remain fully reachable and operable by anyone with sufficient technical knowledge. This open, permissionless nature is precisely what defines and empowers public blockchains.

Conclusion

I would like to thank the European Data Protection Board once again for its efforts in addressing the complex interplay between data protection and emerging technologies. I hope that the observations and perspectives provided in this review contribute meaningfully to the ongoing discussion around the application of the GDPR in decentralized environments.

Should the EDPB have any questions or wish to discuss any of the points raised, I would be pleased to provide further clarification. I can be reached via email I have provided during the submission of this opinion piece.

Best Regards,
Esen Esener, LLM., LL.M